

# On the cryptanalysis of Fridrich's chaotic image encryption scheme

Eric Yong Xie<sup>a</sup>, Chengqing Li<sup>a,\*</sup>, Simin Yu<sup>b</sup>, Jinhu Lü<sup>c</sup>

<sup>a</sup> Hunan Province Cooperative Innovation Center for Wind Power Equipment and Energy Conversion,  
College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China

<sup>b</sup> College of Automation, Guangdong University of Technology, Guangzhou 510006, Guangdong, China

<sup>c</sup> Academy of Mathematics and Systems Sciences, Chinese Academy of Sciences, Beijing 100190, China

## Abstract

Utilizing complex dynamics of chaotic maps and systems in encryption was studied comprehensively in the past two and a half decades. In 1989, Fridrich's chaotic image encryption scheme was designed by iterating chaotic position permutation and value substitution some rounds, which received intensive attention in the field of chaos-based cryptography. In 2010, Solak *et al.* proposed a chosen-ciphertext attack on the Fridrich's scheme utilizing influence network between cipher-pixels and the corresponding plain-pixels. Based on their creative work, this paper scrutinized some properties of Fridrich's scheme with concise mathematical language. Then, some minor defects of the real performance of Solak's attack method were given. The work provides some bases for further optimizing attack on the Fridrich's scheme and its variants.

**Keywords:** Chaotic encryption, chosen-ciphertext attack, cryptanalysis, differential attack.

## 1. Introduction

The complex dynamics of chaotic systems attracts researchers to utilize them as a new way to design secure and efficient encryption schemes [1, 2, 3, 4, 5, 6]. The first chaos-based encryption scheme was proposed in 1989 [7], where a chaotic equation

$$g(x) = (\beta + 1)(1 + 1/\beta)^\beta x(1 - x)^\beta, \quad \beta \in [1, 4] \quad (1)$$

was derived to generate pseudo-random number sequence and then mask the plaintext with modulo addition. Soon after publication of [7], it was pointed out that period of the sequence generated by iterating Eq. (1) may be very short, especially when it is implemented with small computing precision, which may seriously compromise the security level of the scheme [8]. Some special defects and properties of chaotic systems may facilitate cryptanalysis of chaos-based encryption schemes, e.g. chaotic synchronization [9], chaotic ergodicity [10], and parameter identification of chaotic system [11]. The inadequate combination of chaotic dynamics and encryption architectures makes the complexity of recovering its secret key from some pairs of plain-texts and the corresponding cipher-texts, encrypted with the same secret key, lower than that of brute-force

attack [12, 13, 14, 15]. Some general rules on evaluating security of chaos-based encryption schemes can be found in [16, 17].

As quantitatively analyzed in [18, 19], any position permutation-only encryption scheme can be efficiently broken with only  $O(\lceil \log_L(H \cdot W) \rceil)$  known/chosen plaintexts and the computational complexity of magnitude  $O(H \cdot W \cdot \lceil \log_L(H \cdot W) \rceil)$ , where  $L$  denotes the number of different gray-values of the plaintexts, and  $H \times W$  (height×width) is the size of the encryption scheme's *permutation domain*, whose every element denotes the mapping relation between the relative position of a permuted element in the plaintext and that in the corresponding ciphertext. As suggested in [20], iterating position permutation and value substitution sufficient rounds can make an encryption scheme very strong against all kinds of attacks. Considering significant impact of the structure of Fridrich's scheme on a great number of chaotic encryption schemes, Solak's chosen-ciphertext attack method proposed in [21] can be considered as a breakthrough in the field of chaotic cryptanalysis.

According to the record of *Web of Science*, both papers [22] and [23] have been cited more than 500 times up to Aug 2016. Inspired by using space network (function graph) for attacking hash function in [24], we re-summarized some properties of Fridrich's chaotic image encryption scheme with the methodology of complex networks (binary matrix). Then, we further evaluated the real

\*Corresponding author.

Email address: DrChengqingLi@gmail.com (Chengqing Li)

performance of Solak's chosen-ciphertext attack method and found that it owns some minor defects. In addition, the performance of extension of the attack idea to Chen's scheme proposed in [23, 25] was also briefly evaluated.

The rest of this paper is organized as follows. Section 2 concisely introduces Fridrich's chaotic image encryption scheme. Our cryptanalytic results of the scheme are presented in Sec. 3 in detail. The last section concludes the paper.

## 2. Fridrich's chaotic image encryption scheme

The plaintext encrypted by Fridrich's chaotic image encryption scheme is a gray-scale image of size  $H \times W$ <sup>1</sup>, which can be denoted by a sequence of length  $HW$  in domain  $\mathbb{Z}_{256}$ ,  $\mathbf{I} = [I(i)]_{i=0}^{HW-1}$ , by scanning it in the raster order. The corresponding cipher-image is  $\mathbf{I}' = [I'(i)]_{i=0}^{HW-1}$ . The framework of Fridrich's scheme can be described as follows.

- *Encryption procedure:*

1) *Position Permutation:* for  $i = 0 \sim HW - 1$ , do

$$\mathbf{I}^*(w(i)) = \mathbf{I}(i), \quad (2)$$

where *permutation matrix*  $\mathbf{W} = \{w(i)\}_{i=0}^{HW-1}$  satisfies  $w(i_1) \neq w(i_2)$  for any  $i_1 \neq i_2$ .

2) *Value Substitution:* for  $i = 0 \sim HW - 1$ , carry out substitution function

$$\mathbf{I}'(i) = \mathbf{I}^*(i) \boxplus g(\mathbf{I}'(i-1)) \boxplus h(i), \quad (3)$$

where  $a \boxplus b = (a + b) \bmod 256$ ,  $g: \mathbb{Z}_{256} \rightarrow \mathbb{Z}_{256}$  is a fixed nonlinear function,  $\mathbf{H} = \{h(i)\}_{i=0}^{HW-1}$  is a pseudo-random number sequence, and  $\mathbf{I}'(-1)$  is a pre-defined parameter  $c$ .

3) *Repetition:* set  $\mathbf{I} = \mathbf{I}'$  and repeat the above two steps for  $r-1$  times, where  $r$  is a predefined positive integer.

- *Decryption procedure:* it is similar to the encryption procedure except that the two main encryption steps are carried out in a reverse order, the permutation matrix  $\mathbf{W}$  is replaced by its inverse, and Eq. (3) is replaced by equation

$$\mathbf{I}^*(i) = \mathbf{I}'(i) \boxminus g(\mathbf{I}'(i-1)) \boxminus h(i), \quad (4)$$

where  $(a \boxminus b) = (a - b + 256) \bmod 256$ .

Incorporating Eq. (2) into Eq. (3), one can get

$$\mathbf{I}'(i) = \mathbf{I}(w^{-1}(i)) \boxplus g(\mathbf{I}'(i-1)) \boxplus h(i), \quad (5)$$

where  $\mathbf{W}^{-1} = \{w^{-1}(i)\}_{i=0}^{HW-1}$  is the inverse of  $\mathbf{W}$ . Combining Eq. (2) and Eq. (4), one has

$$\mathbf{I}(i) = \mathbf{I}'(w(i)) \boxminus g(\mathbf{I}'(w(i)-1)) \boxminus h(w(i)). \quad (6)$$

Since publication of [22], a great number of methods have been proposed to modify some elements of the framework of Fridrich's scheme from various aspects, such as using novel methods to generate the permutation matrix; defining new concrete function  $g$  in Eq. (3); changing the involved operations in the substitution function.

## 3. Cryptanalysis

To facilitate further security analysis of Fridrich's scheme, we re-present some properties of Fridrich's scheme reported in [21, Sec. 3] with the methodology of matrix theory. Some critical details are appended to make their description complete, especially the conditions in Property 3 were found by us in the experiments.

### 3.1. Some properties of Fridrich's scheme

**Property 1.** *There exists influence path between the  $i$ -th pixel of  $\mathbf{I}$  and the  $j$ -th one of  $\mathbf{I}'$  (the value of the former may be influenced by that of the latter) if and only if*

$$(\widehat{\mathbf{T}})^r(i, j) > 0,$$

where  $\widehat{\mathbf{T}} = \mathbf{P} \cdot \mathbf{T}$ ,

$$\mathbf{P}(i, j) = \begin{cases} 1 & \text{if } j = w(i); \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\mathbf{T} = \begin{pmatrix} 1 & & & & 0 \\ 1 & 1 & & & \\ & 1 & 1 & & \\ 0 & & \ddots & \ddots & \\ & & & 1 & 1 \end{pmatrix}_{HW \times HW}.$$

*Proof.* First, we consider the case when  $r$  is equal to one. Observing Eq. (4), one can see that relation between  $\mathbf{I}^*$  and  $\mathbf{I}'$  can be presented by the matrix  $\mathbf{T}$ : the value of the  $i$ -th pixel of  $\mathbf{I}^*$  is influenced by that of the  $j$ -th one of  $\mathbf{I}'$  if  $\mathbf{T}(i, j) > 0$  and not otherwise, where

$$\mathbf{T}(i, j) = \begin{cases} 1 & \text{if } 0 \leq i - j \leq 1; \\ 0 & \text{otherwise.} \end{cases} \quad (7)$$

<sup>1</sup>For simplicity, use  $HW$  to denote  $H \cdot W$ .

Permutation operation in Eq. (2) can be presented as multiplication of the permuted vector and an elementary matrix:

$$\mathbf{I}^* = \mathbf{I} \cdot \mathbf{P}. \quad (8)$$

So, one can assure that the value of the  $i$ -th pixel of  $\mathbf{I}$  may be influenced by that of the  $j$ -th pixel of  $\mathbf{I}^*$  if  $\widehat{\mathbf{T}}(i, j) > 0$  and not otherwise. Note that the influence may be cancelled by the modulo operation in Eq. (6). If  $r > 1$ , one can easily derive that the value of  $i$ -th pixel of  $\mathbf{I}$  is influenced by that of the  $j$ -th one of  $\mathbf{I}^*$  if and only if

$$(\widehat{\mathbf{T}})^r(i, j) > 0.$$

□

**Property 2.** If  $w(x) + 1 = w(y)$ ,  $w(y) + 1 = w(z)$ , difference of two sets of entries of  $(\widehat{\mathbf{T}})^r$  is a subset of another similar set:

$$\{j | (\widehat{\mathbf{T}})^r(y, j) > 0\} \setminus \{j | (\widehat{\mathbf{T}})^r(x, j) > 0\} \subset \{j | (\widehat{\mathbf{T}})^r(z, j) > 0\}, \quad (9)$$

where  $x, y, z \in \mathbb{Z}_{HW}$ .

*Proof.* From the definition of matrix multiplication and matrix (7), one has

$$\begin{aligned} & (\widehat{\mathbf{T}})^r(x, j) \\ &= \sum_{k=1}^{HW} \widehat{\mathbf{T}}(x, k) \cdot (\widehat{\mathbf{T}})^{r-1}(k, j) \\ &= \sum_{k=1}^{HW} \sum_{l=1}^{HW} \mathbf{P}(x, l) \cdot \mathbf{T}(l, k) \cdot (\widehat{\mathbf{T}})^{r-1}(k, j) \\ &= \sum_{k=1}^{HW} \mathbf{P}(x, w(x)) \cdot \mathbf{T}(w(x), k) \cdot (\widehat{\mathbf{T}})^{r-1}(k, j) \\ &= \sum_{k=1}^{HW} \mathbf{T}(w(x), k) \cdot (\widehat{\mathbf{T}})^{r-1}(k, j). \end{aligned} \quad (10)$$

As  $\mathbf{T}(w(x), k) = 0$  when  $k \notin \{w(x) - 1, w(x)\}$ , one can get the following two points when  $r > 1$ :

- $(\widehat{\mathbf{T}})^r(x, j) > 0$  if and only if  $(\widehat{\mathbf{T}})^{r-1}(w(x), j) > 0$  or  $(\widehat{\mathbf{T}})^{r-1}(w(x) - 1, j) > 0$  when  $w(x) \neq 0$ ;
- $(\widehat{\mathbf{T}})^r(x, j) > 0$  if and only if  $(\widehat{\mathbf{T}})^{r-1}(w(x), j) > 0$  when  $w(x) = 0$ .

This means that

$$\{j | (\widehat{\mathbf{T}})^r(x, j) > 0\} = \begin{cases} \{j | (\widehat{\mathbf{T}})^{r-1}(w(x), j) > 0\} & \text{if } w(x) = 0; \\ \{j | (\widehat{\mathbf{T}})^{r-1}(w(x), j) > 0\} \cup \{j | (\widehat{\mathbf{T}})^{r-1}(w(x) - 1, j) > 0\} & \text{otherwise.} \end{cases} \quad (11)$$

Since  $w(y) \neq 0$ ,  $w(z) \neq 0$ , one can deduce the following two sets of equations similarly:

$$\begin{aligned} & \{j | (\widehat{\mathbf{T}})^r(y, j) > 0\} \\ &= \{j | (\widehat{\mathbf{T}})^{r-1}(w(y), j) > 0\} \cup \{j | (\widehat{\mathbf{T}})^{r-1}(w(y) - 1, j) > 0\}, \\ &= \{j | (\widehat{\mathbf{T}})^{r-1}(w(y), j) > 0\} \cup \{j | (\widehat{\mathbf{T}})^{r-1}(w(x), j) > 0\}, \end{aligned} \quad (12)$$

and

$$\begin{aligned} & \{j | (\widehat{\mathbf{T}})^r(z, j) > 0\} \\ &= \{j | (\widehat{\mathbf{T}})^{r-1}(w(z), j) > 0\} \cup \{j | (\widehat{\mathbf{T}})^{r-1}(w(z) - 1, j) > 0\}, \\ &= \{j | (\widehat{\mathbf{T}})^{r-1}(w(z), j) > 0\} \cup \{j | (\widehat{\mathbf{T}})^{r-1}(w(y), j) > 0\}. \end{aligned} \quad (13)$$

Using relation between absolute complement and relative complement of a set, one can obtain difference of the left parts of Eq. (12) and Eq. (11),

$$\begin{aligned} & \{j | (\widehat{\mathbf{T}})^r(y, j) > 0\} \setminus \{j | (\widehat{\mathbf{T}})^r(x, j) > 0\} \\ &= \begin{cases} \{j | (\widehat{\mathbf{T}})^{r-1}(w(y), j) > 0\} \cap \{j | (\widehat{\mathbf{T}})^r(x, j) = 0\} & \text{if } w(x) = 0; \\ \{j | (\widehat{\mathbf{T}})^{r-1}(w(y), j) > 0\} \cap \{j | (\widehat{\mathbf{T}})^{r-1}(w(x), j) = 0\} \cup \{j | (\widehat{\mathbf{T}})^{r-1}(w(x) - 1, j) = 0\} & \text{otherwise.} \end{cases} \end{aligned}$$

For either case of the above equation, one can get

$$\{j | (\widehat{\mathbf{T}})^r(y, j) > 0\} \setminus \{j | (\widehat{\mathbf{T}})^r(x, j) > 0\} \subset \{j | (\widehat{\mathbf{T}})^r(z, j) > 0\} \quad (14)$$

by observing the right part of Eq. (13). □

**Corollary 1.** If  $w(x) = 0$ ,  $w(y) = 1$ , then

$$\{j | (\widehat{\mathbf{T}})^r(x, j) > 0\} \subset \{j | (\widehat{\mathbf{T}})^r(y, j) > 0\}. \quad (15)$$

*Proof.* This corollary can be easily proofed by comparing Eq. (11) and Eq. (12). □

**Property 3.** If  $w(0) \neq 1$ ,  $|w(x_1) - w(x_2)| \neq 1$  for any  $x_1, x_2$  satisfying  $|x_1 - x_2| \in \{1, \dots, 2^{r-1} - 1\}$ , one has

$$w(x) = 0,$$

where the  $x$ -th row of  $(\widehat{\mathbf{T}})^r$  is its row vector containing minimal number of non-zero element, i.e.,

$$||j | (\widehat{\mathbf{T}})^r(x, j) > 0|| = \min \{ ||j | (\widehat{\mathbf{T}})^r(i, j) > 0|| \}_{i=0}^{HW-1}, \quad (16)$$

and  $r \geq 2$ .

*Proof.* As shown in Fig. 1, there exist and only exist three basic patterns for reducing the number of influencing cipher-pixels for a plain-pixel. If  $|w(x_1) - w(x_2)| \neq 1$  for any  $x_1, x_2$  satisfying  $|x_1 - x_2| \in \{1, \dots, 2^{r-1} - 1\}$ , the first two patterns in Fig. 1 can be excluded. Furthermore, the third one can be eliminated if  $w(0) \neq 1$ . (A concrete counter example is shown in Fig. 2.) Under the given condition in this property, there is only one influence path between any pair of cipher-pixel and plain-pixel. So, the  $x$ -th row of  $(\hat{\mathbf{T}})^r$  has  $2^{r-1}$  non-zero elements while other rows all have  $2^r$  non-zero elements. Then, one can correctly recover  $w(x) = 0$  by checking condition (16).  $\square$

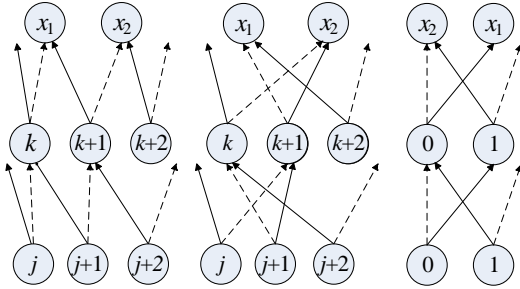


Figure 1: Three basic patterns for reducing incoming influence paths of a plain-pixel, where the solid arrow indicates influence caused by  $\mathbf{I}'(w(i))$  and the dashed arrow denotes that caused by  $\mathbf{I}'(w(i) - 1)$ , and the symbol inside a circle denotes the index number of pixel (the same hereinafter).

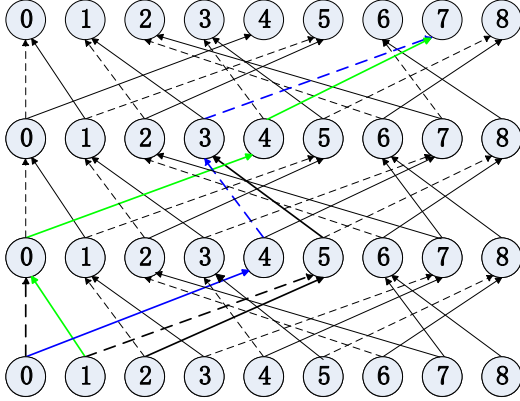


Figure 2: A counterexample on Property 3, where  $\mathbf{W} = [1, 3, 7, 5, 0, 2, 8, 4, 6]$ , and  $r = 3$ .

### 3.2. Description of Solak's chosen-ciphertext attack

To facilitate the discuss in the next subsection, we concisely describe the process of Solak's chosen-ciphertext attack method given in [21]. Let  $\hat{\mathbf{W}}^{-1} = \{\hat{w}^{-1}(i)\}_{i=0}^{HW-1}$  denote the estimated version of  $\mathbf{W}^{-1}$ . After recovering the approximate version of the influence matrix between cipher-text

and the corresponding plain-text, the Solak's attack method prunes the search space of size  $HW!$  (factorial of  $HW$ ) with the following steps:

- *Step 1)* Set  $\hat{w}^{-1}(0) = x_0$ , where  $x_0$  is the row number satisfying condition (16) itself.
- *Step 2)* Let  $\hat{w}^{-1}(1) = x_1$ , where  $x_1 \in \mathbf{A} \setminus \mathbf{B}$ ,  $\mathbf{A}$  is the right-hand set in condition (15) with  $x = x_0$ , and  $\mathbf{B} = \{x_0\}$ .
- *Step 3)* For  $i = 2 \sim HW - 1$ , let  $\hat{w}^{-1}(i) = x_i$ , where  $x_i \in \mathbf{A} \setminus \mathbf{B}$ ,  $\mathbf{A}$  is the right-hand set in condition (9) with  $x = i - 1$ ,  $y = i$ , and  $\mathbf{B} = \{x_j\}_{j=0}^{i-1}$ . If  $\mathbf{A}$  is empty, one can assure that the current value of  $\hat{w}^{-1}(i - 1)$  is wrong and process the search with its another candidate value.
- *Step 4)* Repeat the above steps iteratively till variable  $i$  reaches the maximal value,  $HW - 1$ .

### 3.3. Real performance of Solak's chosen-ciphertext attack

Observing Eq. (6), one can see that the  $i_0$ -th plain-pixel can be only influenced by one cipher-pixel in each encryption round if  $w(i_0) = 0$ . After accumulation of  $r$  rounds of encryption, the number of cipher-pixels influencing the  $i_0$ -th plain-pixel is smaller than that influencing other plain-pixels in a very high probability, which serves as the basis of *Step 1*). The scope of the former is  $[1, 2^{r-1}]$ . In contrast, the scope of the latter is  $[r + 1, 2^r]$ , whose lower bound can be achieved when there exist  $x$  and  $t = r$  satisfying  $|w(x + i + 1) - w(x + i)| = 1$  for  $i = 0 \sim t - 1$ . Observing the right part of Fig. 3, one can see that the number of cipher-pixels influencing the  $x$ -th plain-pixel shifts from  $r + 1$  to  $2^r$  monotonously when  $t$  is increased from 0 to  $r$ . Property 3 only presents an extreme condition assuring the estimation in *Step 1*) is definitely right. Interestingly, the condition in Property 3 is very similar to the problem of neighbors remain neighbors after random rearrangements, discussed in [26].

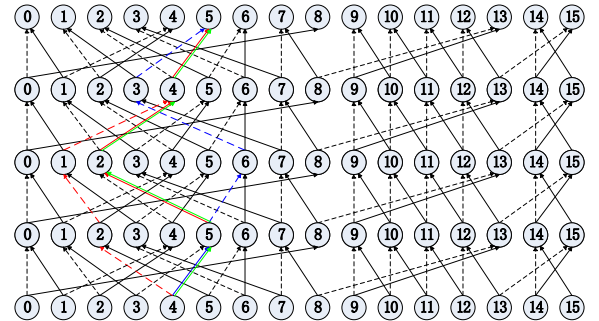


Figure 3: Another counterexample about Property 3.

Now, we give a counterexample to show deficiency of Solak's chosen-ciphertext attack method. When  $\mathbf{W} =$

[1, 3, 5, 7, 2, 4, 6, 8, 0, 10, 11, 12, 13, 9, 15, 14],  $r = 4$ , the influence relation between the cipher-pixels and the corresponding plain-pixels is shown in Fig. 3. Its binary matrix form is presented in Fig. 4, which demonstrates that the 9-th row has least non-zero elements. According to Solak's attack method, one can get  $w(9) = 0$ , which is contradict with the real value. As the initial step has cascaded influence on the succeeding steps, the attack is totally failed under the given secret key.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Figure 4: Obtained influence matrix when  $\mathbf{W} = [1, 3, 5, 7, 2, 4, 6, 8, 0, 10, 11, 12, 13, 9, 15, 14]$ , and  $r = 4$ .

As shown in [21, Sec. 4], when permutation vector  $\mathbf{W} = [8, 7, 5, 11, 0, 10, 13, 14, 6, 2, 9, 1, 15, 4, 3, 12]$  and  $r = 3$ , the permutation vector can be solely recovered with Solak's chosen-ciphertext attack method. However, when it is slightly changed as  $\mathbf{W} = [8, 7, 5, 11, 12, 10, 13, 14, 6, 2, 9, 1, 15, 0, 3, 4]$ , eight possible values are obtained by the attack (See Fig. 5). To verify this point further, we performed Solak's attack on a plaintext of size  $1 \times 32$  with 1,000 randomly assigned  $\mathbf{W}$  and three possible encryption rounds. The following five cases, in terms of attacking results, were counted: 1) the right key is enclosed; 2) the sole result is the right key; 3) both right key and wrong key exist; 4) no any result is obtained; 5) all found results are wrong. Let  $n_1, n_2, n_3, n_4$  and  $n_5$  denote the number of the five cases occurring among 1,000 times random experiments, respectively. The calculated results are shown in Table 1, which demonstrates that the attack results become more worse as  $2^r$  approaches  $MN$  more, which agrees with analysis in the proof of Property 3.

### 3.4. Real performance of extension of Solak's attack to Chen's scheme

In [21, Sec. 5], it was claimed that Solak's chosen-plaintext attack method can be applied to Chen's scheme easily and effectively due to similar structure. However, we found some differences caused by the different basic encryption operations.

[8, 7, 4, 11, 12, 10, 13, 14, 5, 2, 9, 1, 15, 0, 3, 6]  
[8, 7, 5, 11, 12, 10, 13, 14, 4, 2, 9, 1, 15, 0, 3, 6]  
[8, 7, 5, 11, 12, 10, 13, 14, 6, 2, 9, 1, 15, 0, 3, 5]  
[8, 7, 6, 11, 12, 10, 13, 14, 5, 2, 9, 1, 15, 0, 3, 4]  
[9, 10, 12, 6, 5, 7, 4, 3, 11, 15, 8, 1, 2, 0, 14, 13]  
[9, 10, 11, 6, 5, 7, 4, 3, 12, 15, 8, 1, 2, 0, 14, 13]  
[9, 10, 13, 6, 5, 7, 4, 3, 12, 15, 8, 1, 2, 0, 14, 11]  
[9, 10, 12, 6, 5, 7, 4, 3, 13, 15, 8, 1, 2, 0, 14, 11]

Figure 5: The results of Solak's attack when  $\mathbf{W} = [8, 7, 5, 11, 12, 10, 13, 14, 6, 2, 9, 1, 15, 0, 3, 4]$ .

Table 1: The number of five possible cases occurring among 1,000 random secret keys.

$r$	2	3	4
$n_1$	1000	957	814
$n_2$	964	867	571
$n_3$	36	90	243
$n_4$	0	43	180
$n_5$	0	0	6

In [23, 25], Chen's scheme changes Eq. (3) as

$$\mathbf{I}'(i) = h(i) \oplus [\mathbf{I}^*(i) \boxplus h(i)] \oplus \mathbf{I}'(i-1).$$

Accordingly, Eq. (4) becomes

$$\mathbf{I}^*(i) = (h(i) \oplus \mathbf{I}'(i) \oplus \mathbf{I}'(i-1)) \boxminus h(i). \quad (17)$$

Combing Eq. (2) and Eq. (17), one has

$$\mathbf{I}(i) = (h(w(i)) \oplus \mathbf{I}'(w(i)) \oplus \mathbf{I}'(w(i)-1)) \boxminus h(w(i)). \quad (18)$$

When  $\mathbf{W} = [1, 3, 5, 7, 2, 4, 6, 8, 0, 10, 11, 12, 13, 9, 15, 14]$ , and  $r = 4$ , the number of different influence paths between a cipher-pixel and any plain-pixel is shown in Fig. 6. Due to the bitwise exclusive or (XOR) operation used in Eq. (17), the influence of a cipher-pixel on a influenced plain-pixel may be cancelled when there is multiple influence paths between them. So, some influence paths can not be recovered. Note that even error of one element of the influence matrix may fail a attacking step based on the sets comparison and disable the following steps due to the cascading influence. More discussions on composite function of modulo addition and XOR operation can be found in [27, Sec. 3.1]. Figure 7 shows the obtained influence matrix by changing every cipher-pixel with the fixed value one, which has six unrecovered influence paths. As the recovered influence matrix of sufficient accuracy is requisite condition for success of the Solak's attack method, one has to improve its correct ratio by changing cipher-pixel with the other values (more cipher-images).

Note that equivalent version of position permutation and value substitution of 1-round version Chen's scheme was

1	2	2	2	2	2	2	2	1	0	0	0	0	0	0	0
1	1	2	2	2	2	2	2	1	0	0	0	0	0	0	0
0	1	2	2	3	3	2	2	1	0	0	0	0	0	0	0
2	2	1	1	1	1	2	2	1	0	0	0	0	0	0	0
0	2	3	2	2	2	2	2	1	0	0	0	0	0	0	0
1	1	1	2	3	2	2	2	1	0	0	0	0	0	0	0
0	1	2	2	2	3	3	2	1	0	0	0	0	0	0	0
3	2	1	1	0	0	0	1	1	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	1	4	6	4	1	0	0	0
0	0	0	0	0	0	0	0	1	1	1	4	6	3	0	0
1	0	0	0	0	0	0	0	2	3	1	1	4	3	0	0
2	1	0	0	0	0	0	0	1	3	3	1	1	1	0	0
1	1	1	1	0	0	0	0	0	1	3	3	1	0	0	0
1	0	0	0	0	0	0	0	1	2	1	0	0	2	5	3
1	1	0	0	0	0	0	0	1	2	2	1	0	1	3	2

Figure 6: The number of different influence paths between the  $i$ -th cipher-pixel and the  $j$ -th plain-pixel, where  $\mathbf{W} = [1, 3, 5, 7, 2, 4, 6, 8, 0, 10, 11, 12, 13, 9, 15, 14]$ , and  $r = 4$ .

1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
1	1	1	1	0	0	1	1	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	1	0	1	1	1	0	0	0
0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0
1	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0
1	1	0	0	0	0	0	0	1	1	1	1	1	0	0	0
1	1	1	1	0	0	0	0	0	1	1	1	1	0	0	0
1	0	0	0	0	0	0	0	1	0	1	0	0	0	1	1
1	1	0	0	0	0	0	0	1	0	0	1	0	1	1	0

Figure 7: Obtained influence matrix when  $\mathbf{W} = [1, 3, 5, 7, 2, 4, 6, 8, 0, 10, 11, 12, 13, 9, 15, 14]$ , and  $r = 4$ .

successfully recovered with some chosen-plaintexts in [28]. Its weak sensitivity with respect to changes of secret key and plaintext was demonstrated in detail in [29].

#### 4. Conclusion

Based on the work in [21], this paper formulated some properties of Fridrich's chaotic image encryption scheme with matrix theory and reported some minor defects of Solak's chosen-ciphertext attack method on it. The work may help designers of chaotic encryption schemes to realize fundamental importance of the underlying encryption architecture for security performance [30]. The following problems on cryptanalyzing Fridrich's chaotic image encryption scheme deserve further investigation: decreasing the required number of chosen-ciphertext with the special properties of the influence matrix between cipher-pixels and the corresponding plain-pixels; reducing computational complexity of the chosen-ciphertext attack; disclosing the influence matrix under the scenario of known/chosen-plaintext attack.

#### Acknowledgement

This research was supported by Hunan Provincial Natural Science Foundation of China (No. 2015JJ1013), Scientific Research Fund of Hunan Provincial Education Department (No. 15A186), and the National Natural Science Foundation of China (No. 61532020).

#### References

- [1] T. Xiang, K.-W. Wong, X. Liao, Selective image encryption using a spatiotemporal chaotic system, *Chaos* 17 (2) (2007) art. no. 023115.
- [2] H. Liu, Y. Liu, Security assessment on block-cat-map based permutation applied to image encryption scheme, *Optics & Laser Technology* 56 (2014) 313–316. doi:10.1016/j.optlastec.2013.09.012.
- [3] Z. Lin, S. Yu, J. Lu, S. Cai, G. Chen, Design and ARM-embedded implementation of a chaotic map-based real-time secure video communication system, *IEEE Transactions on Circuits and Systems for Video Technology* 25 (7) (2015) 1203–1216.
- [4] Y. Zhou, Z. Hua, C.-M. Pun, C. L. P. Chen, Cascade chaotic system with applications, *IEEE Transactions on Cybernetics* 45 (9) (2015) 2001–2012.
- [5] Z. Hua, Y. Zhou, Image encryption using 2D Logistic-adjusted-Sine map, *Information Sciences* 339 (2016) 237–253.
- [6] A. Belazi, A. A. A. El-Latif, S. Belghith, A novel image encryption scheme based on substitution-permutation network and chaos, *Signal Processing* 128 (2016) 155–170.
- [7] R. Matthews, On the derivation of a “chaotic” encryption algorithm, *Cryptologia* 13 (1) (1989) 29–42.
- [8] D. D. Wheeler, Problems with chaotic cryptosystems, *Cryptologia* 13 (3) (1989) 243–250.
- [9] T. Beth, D. E. Lazic, A. Mathias, Cryptanalysis of cryptosystems based on remote chaos replication, in: *Advances in Cryptology—Crypto’94*, Vol. 839 of *Lecture Notes in Computer Science*, 1994, pp. 318–331.
- [10] D. Arroyo, G. Alvarez, S. Li, C. Li, V. Fernandez, Cryptanalysis of a new chaotic cryptosystem based on ergodicity, *International Journal of Modern Physics B* 23 (5) (2009) 651–659.
- [11] E. Solak, Partial identification of lorenz system and its application to key space reduction of chaotic cryptosystems, *IEEE Transactions on Circuits and Systems II: Express Briefs* 51 (10) (2004) 557–560.
- [12] E. Biham, Cryptanalysis of the chaotic-map cryptosystem suggested at Eurocrypt’91, in: *Advances in Cryptology—Crypto’91*, Vol. 547 of *Lecture Notes in Computer Science*, 1991, pp. 532–534.
- [13] D. Arroyo, J. Diaz, F. B. Rodriguez, Cryptanalysis of a one round chaos-based substitution permutation network, *Signal Processing* 93 (5) (2013) 1358–1364.
- [14] C. Li, Y. Liu, T. Xie, M. Z. Q. Chen, Breaking a novel image encryption scheme based on improved hyperchaotic sequences, *Nonlinear Dynamics* 73 (3) (2013) 2083–2089.
- [15] W.-S. Yap, R. C.-W. Phan, W.-C. Yau, S.-H. Heng, Cryptanalysis of a new image alternate encryption algorithm based on chaotic map, *Nonlinear Dynamics* 80 (3) (2015) 1483–1491.
- [16] G. Álvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, *International Journal of Bifurcation and Chaos* 16 (8) (2006) 2129–2151.
- [17] G. Alvarez, J. M. Amigó, D. Arroyo, S. Li, Lessons learnt from the cryptanalysis of chaos-based ciphers, in: L. Kocarev, S. Lian (Eds.), *Chaos-Based Cryptography: Theory, Algorithms and Applications*, Vol. 354 of *Studies in Computational Intelligence*, Springer, 2011, pp. 257–295.

- [18] C. Li, K.-T. Lo, Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, *Signal Processing* 91 (4) (2011) 949–954.
- [19] C. Li, Cracking a hierarchical chaotic image encryption algorithm based on permutation, *Signal Processing* 118 (2016) 203–210.
- [20] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal* 28 (4) (1949) 656–715.
- [21] E. Solak, C. Cokal, O. T. Yildiz, T. Biyikoglu, Cryptanalysis of Fridrich’s chaotic image encryption, *International Journal of Bifurcation and Chaos* 20 (5) (2010) 1405–1413.
- [22] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, *International Journal of Bifurcation and Chaos* 8 (6) (1998) 1259–1284.
- [23] G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos, Solitons & Fractals* 21 (3) (2004) 749–761.
- [24] G. Leurent, T. Peyrin, L. Wang, New generic attacks against hash-based macs, in: *Advances in Cryptology–Asiacrypt 2013*, Vol. 8270 of *Lecture Notes in Computer Science*, 2013, pp. 1–20.
- [25] Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3D chaotic baker maps, *International Journal of Bifurcation and Chaos* 14 (10) (2004) 3613–3624.
- [26] M. Abramson, W. O. J. Moser, Permutations without rising or falling  $\omega$ -sequences, *The Annals of Mathematical Statistics* 38 (4) (1967) 1245–1254.
- [27] C. Li, Y. Liu, L. Y. Zhang, M. Z. Q. Chen, Breaking a chaotic image encryption algorithm based on modulo addition and XOR operation, *International Journal of Bifurcation and Chaos* 23 (4) (2013) art. no. 1350075.
- [28] K. Wang, W. Pei, L. Zou, A. Song, Z. He, On the security of 3D cat map based symmetric image encryption scheme, *Physics Letters A* 343 (6) (2005) 432–439.
- [29] C. Li, G. Chen, On the security of a class of image encryption schemes, in: *Proceedings of 2008 IEEE International Symposium on Circuits and Systems*, 2008, pp. 3290–3293.
- [30] Y. Liu, H. Fan, E. Y. Xie, G. Cheng, C. Li, Deciphering an image cipher based on mixed transformed logistic maps, *International Journal of Bifurcation and Chaos* 25 (13) (2015) Article number 1550188. doi:<http://dx.doi.org/10.1142/S0218127415501886>.